REMARKS

INTRODUCTION

Claims 1-39 were previously pending.

Claim 40 and 41 are added herein.

Claims 3 and 25 are canceled.

Claims 1-2, 4-24, and 26-41 are therefore pending and under consideration.

Claims 1-6, 8-14, 16-17, 20-23, 25-32, and 34-39 stand rejected.

Claims 1, 5, 7, 14, 15, 18, 20, 23, 24, 26-34, and 37 are amended herein.

No new matter has been added.

INTERVIEW SUMMARY

Applicant thanks the Examiner for the in-person Interview of May 9, 2008. During the Interview Applicant explained several aspects of the present invention and also the prior art references. In particular, Applicant noted that Buch is for end-to-end user authentication, and therefore does not relate to specifically signing routing related headers or doing so by a SIP node that is routing a SIP message from one SIP node to another SIP node.

OBJECTED-TO CLAIMS

Claim 7

Claim 7 is amended into independent form and as indicated by the Examiner is allowable.

Claim 15

Claim 15 is amended into independent form and as indicated by the Examiner is

allowable. Note that for clarity "fourth signature" has been changed to "other signature". Allowance of claim 15 is respectfully requested.

Claim 34

Claim 34 is amended into independent form and as indicated by the Examiner is allowable. Some minor changes have been made for clarity without changing the scope of the claim; "for the top-listed" has been changed to "topmost" and "selected from" has been changed to "is one of". Allowance of claim 34 is respectfully requested

REJECTION UNDER 35 USC § 101

Claims 25-31 stand rejected as being directed to non-statutory subject matter. In particular, the rejection states that "[t]he claim is directed to a nonstatutory subject matter because the claims are not written in terms of 'computer' readable medium, stored with, embodied with or encoded with a "computer" program or computer executable instructions".

Claim 25 is canceled in the present response. Claims 26-31 are amended to claim a "computer storage medium" rather than a "computer readable medium". Based at least on the disclosure found on page 41 of the present application describing a "computer storage medium", Applicant respectfully requests reconsideration and withdrawal of the rejection of claims 26-31.

REJECTION UNDER 35 USC § 102

Claims 1-2, 25-29, 30, and 37 are rejected under 35 U.S.C. 102(b) as being anticipated by Buch (US Publication 2003/0217165).

Overview of Buch

Buch discusses a system for end-to-end SIP user authentication. Because Buch is for

end-to-end authentication (i.e., authentication by either the caller or callee endpoints), Buch cannot meet various features of the claims discussed below.

Referring to Figure 2 of Buch, it can be seen that only the user computers (endpoints) 84 and 142 sign messages. The signatures in Buch are for verifying the content and identity of a message being sent. As noted in paragraph 0027, "When the SIP client 72 sends the INVITE message 82, it includes in the message a digital signature 100 that is generated using a private key of the user [or a session key]. As shown in FIG. 2, the user Ann has a public key 110 and the associated private key 112... Typically, the process of generating the digital signature 100 involves generating a one-way hash (or digest) from selected portions of the SIP message, and encoding the hash with the private key 112 to produce the digital signature 100." Either the caller or callee may generate the signature. As noted in Buch's Abstract, "The SIP request message is sent with a digital signature generated with a private key of the sender and may include a certificate of the sender".

Claim 1

Amended claim 1 recites a SIP node that receives a "SIP request including a message header including data indicative of network routing locations." Claim 1 also requires "editing the data at the SIP node" and "generating a signature based upon at least a portion of the message header including the edited data." Therefore, claim 1 requires that data indicative of network routing locations that is included in a message header (e.g. VIA and RECORD-ROUTE information), which is edited at each node, be included in the signature.

In contrast to claim 1, Buch's endpoint user computers generate and add signatures only based on information that is not altered by intermediate SIP nodes. The Office Action acknowledges that Buch does not disclose use of data indicative of network routing locations in

a signature. Office Action at 9. Secondly, and as noted in Buch, paragraph 0044, "Whether a header should be included in the signature or not may depend on whether it will be modified by the SIP proxy. For instance, headers that should or must be modified by the SIP proxy should not be included in the signature". Buch therefore teaches that network routing information, which is edited at each SIP node, should not be used in a signature; Buch therefore teaches away from use in any combination (e.g. with Tsuzuki) to arrive at claim 1.

Withdrawal of the rejection of claim 1 is respectfully requested.

Claim 26

Claim 26 recites forming an encrypted session key ("encrypting the session key with the private key") and "generating, with the public key, a key signature based on the encrypted session key". In other words, the session key is encrypted and then signed using the public key. This can protect the session key from other servers. A receiver of the encrypted session key and signature thereof can use the signature to verify the encrypted session key before decrypting it.

The rejection cites paragraph 0028 of Buch. However, this portion of Buch discusses "the authentication process". Claim 26 relates not to authenticating but rather to encrypting a session key and signing the encrypted key with a public key. Nonetheless, even if the decryption/authentication process of paragraph 0028 is reversed to a corresponding encryption/signing, it can be seen that such encryption/signing differs from claim 26. For example, the "digital signature" of paragraph 0028 is not a signature of a session key. The signature 100 is generated by a "one-way hash (or digest) from selected portions of the SIP message". Buch does not sign an encrypted session key, rather it signs a *message* by using a public key to encrypt a hash/digest of the message.

Withdrawal of the rejection is respectfully requested.

Should the rejection be maintained, Applicant respectfully requests the Examiner to explain exactly what in Bush is deemed to be analogous so a signed encrypted session key.

Claim 32

Claim 32 recites a SIP request with "a plurality of SIP headers". Claim 32 also recites that the SIP request has "data representing a digital signature generated by signing a portion of the SIP headers", which is "appended to one of the SIP headers" (either a VIA, FROM, TO, RECORD-ROUTE, CALL-ID, or CSeq header). In other words, one of these headers has a digital signature appended to it.

In contrast, the digital signature of Buch is either added to a new header or included in the message body. As noted in paragraph 0006 of Buch, "for including the digital signature in the SIP message", Buch will:

> **create a header**, such as a new Authorization (for an end client) or Proxy Authorization header (for an intermediate SIP server), in the SIP message for carrying the signature and optionally the certificate. **An alternative** scheme in accordance with the invention for carrying a digital signature in the SIP request is to **include the signature** ... **in the multipart message body** of the SIP request message, preferably formatted according to the Secure/Multipurpose Internet Mail Extensions (S/MIME) standard.

Buch does not discuss or suggest appending a signature to a VIA, FROM, TO, RECORD-ROUG, CALL-ID, or CSEQ header.

Withdrawal of the rejection is respectfully requested.

REJECTION UNDER 35 USC § 103

Claims 3-6, 8-14, 16-17, 20-23, 32, 34-36, and 38-39 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Buch in view of Tsuzuki (US2004/0246991).

Improper Combination

The rejection modifies Buch with Tsuzuki in part to "in order to prevent request looping and ensure replies take the same path as the requests". However Tsuzuki is for there is no information or art of record which suggests that looping or path consistency was of any concern prior to the present invention. It appears that this motivation for combining the references comes from Applicant's specification and therefore constitutes improper hindsight. Furthermore, the rejection provides no reasoning on how the proposed modification would actually prevent looping or ensure path consistency. Tsuzuki only provides mechanisms to facilitate IPv4 to IPv6 address translation. Buch only signs a message. It is not clear how either reference individually, or the references combined, would prevent looping or ensure path consistency.

Claims 11-14, 16, 17, and 20-23

Claims 11-14, 16, 17, and 20-23 are rejected based on an assumption that it is inherent to have a second signature, third, or fourth. However, it appears that Buch discusses only one signature in a message. The referenced paragraph 0036 only mentions that there are two different ways to include the single message signature. Applicant respectfully requests the Examiner to withdraw the rejection or explain why the mentioned features are inherent in Buch.

Withdrawal of the rejection is respectfully requested.

CONCLUSION

The present application is in condition for allowance. A prompt action to such end is requested.

Should any fees be required in connection with this document, the Commissioner is authorized to charge those fees to Deposit Account No. 50-0463.

If the Examiner believes a telephone interview would be helpful to expedite prosecution, the Examiner is invited to contact Applicant's undersigned representative at the telephone number below.

Respectfully submitted,

Microsoft Corporation

Date: 7/15/2008

By: /James T. Strom/

James T. Strom, Reg. No.: 48,702
Attorney for Applicants
Direct telephone 425-939-0781